



FortiProxy Troubleshooting

Viswabharath
EMEA Escalation Team



Introduction



FortiProxy Secure Web Gateway



- High Performance and Scalability Proxy
- Dedicated Secure Web Gateway Solution
- Pay As You Grow License
- Multi-Layered Detection to prevent threats
- Authenticated Web Application Control
- Wan Optimization and Advanced Caching



SSL INSPECTION



- Powerful hardware
- Removes blind spots in encrypted traffic
- Multiple inspection methods

MULTI-LAYERED PROTECTION



- Integration with proven FortiGuard Threat Intelligence
- Integration with FortiSandbox

AUTHENTICATED ACCESS



- Granular application control policies
- Activity monitoring
- Restricts access to social websites using user or group identity

FortiProxy Appliance Lineup



Specification	FPX400E	FPX2000E	FPX4000E
Base Features	Advanced Caching and WAN Optimization		
User License	500-4000 Users	2,500-25,000 Users	15,000-50,000 Users
Service License (All-Inclusive)	Web Filtering, DNS Filtering, Application Control, DLP, AV, IPS, Botnet (IP/Domain) and FortiSandbox Cloud		
Ports	4 x 10/100/1000 RJ45	2 x 10/100/1000 RJ45 2 x 10/100/1000 RJ45 bypass 2 x 1GbE SFP 2 x 10GbE SFP+	4 x 10/100/1000 RJ45 2 x 10/100/1000 RJ45 bypass 2 x 1GbE SFP 4 x 10GbE SFP+
Memory	8GB	64GB	128GB
Storage	4TB (2 x 2TB HDD)	8TB (4 x 2TB HDD) (plus 4 x 2TB Optional)	8TB (4 x 2TB HDD) (plus 8 x 2TB Optional)
SSL Hardware	2 x CP9	2 x CP9	2 x CP9
Power Supply	AC power supply (Optional Dual)	Dual AC power supply	Dual AC power supply

All platforms support FIPS 140-2 and Common Criteria



FortiProxy VM Lineup (VM01-VMUL)

Specification	VM01	VM02	VM04	VM08	VM16	VMUL
Base Features	Advanced Caching and WAN Optimization					
User License	100 Users	100 - 500 Users	100 -2,500 Users	100 - 10,000 Users	100 -25,000 Users	100 - 50,000 Users
Hypervisor Support	VMware ESX/ESXi, KVM Platform and Microsoft HyperV					
Service License	SWG Protection Bundle: Web Filtering, DNS Filtering, Application Control, DLP, Antivirus, IPS, Botnet (IP/Domain) and FortiSandbox Cloud					
CPU	2x vCPU	4x vCPU	8x vCPU	16x vCPU	32x vCPU	Unlimited vCPU
Memory	Unlimited (G) x RAM					
Storage	1 Disk	2 Disks	2 Disks	4 Disks	8 Disks	16 Disks
Ports	Up to 10 Interface					



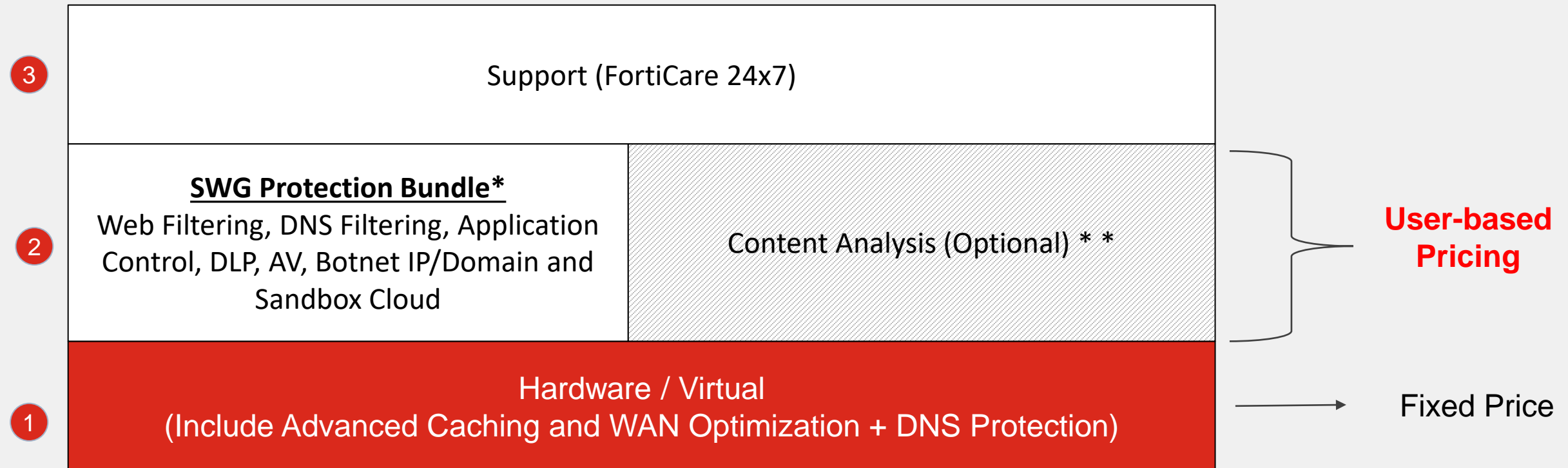


Licensing



Licensing Model

PAYG User Based Licensing – Minimum users required



* Scale up to 50K users depend on HW/VM Model

** Equal to SWG Protection Bundle amount, Real-time analysis of images to detect adult content. Detection of adult content in images uses various patented techniques (not just color-based), including limb and body part detection, body position, and so on. When adult content is detected, such content can be optionally blocked or reported.



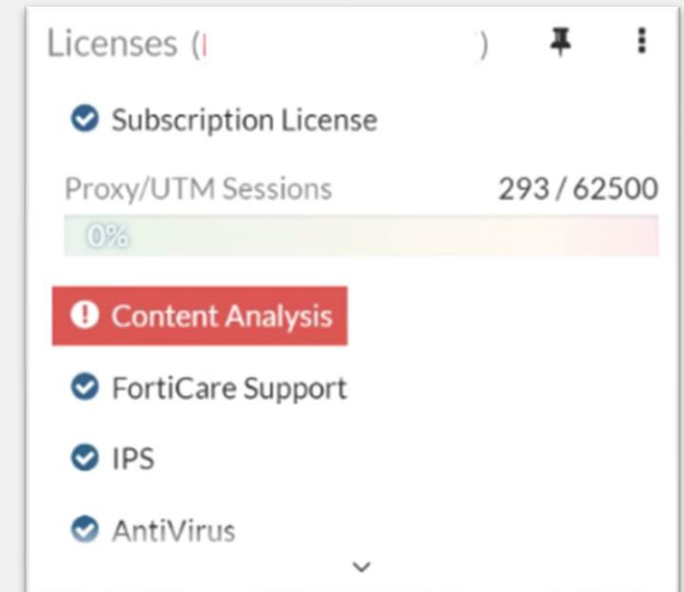
How FortiProxy calculate the number of users/seats?

- FortiProxy give 25 sessions per 1 User License.
i.e. customer purchase 2500 users license, he will be entitled for 62,500 sessions (can be from 1 source IP or from many – up to 62,500 source IPs).
- If the number of users/sessions exceeds the license number, we will block the traffic or bypass security check for the traffic based on the user setting.

```
config system global  
set license-overlimit {bypass | block}
```

bypass - Bypass further traffic when licensed user is reached.

block - Block further traffic when licensed user is reached.



```
# diagnose wad license summary  
Available License Seat: 2500  
Max Licensed Session: 62500  
Current User Count: 75  
Current Licensed Session: 293
```


How FortiProxy calculate the number of users/seats?

License calculation

❖ 1.2.7 & Before

$10000 * 10 = 100000$ sessions

System Information

Hostname FPX4KET318000009

Serial Number FPX4KET318000009

Firmware v1.2.6 build0289 (GA)

Mode NAT (Proxy-based)

Licenses (🇺🇸 96.45.33.88)

☒ Subscription License

Proxy/UTM Sessions 0 / 100000

0%

☒ Content Analysis

```
FPX4KET318000009 # diag wad license summary
Available License Seat: 10000
Max Licensed Session: 100000
Current User Count: 0
Current Licensed Session: 0
```

❖ 1.2.8 and later

$10000 / 25 = 250000$ sessions

System Information

Hostname FPX4KET318000009

Serial Number FPX4KET318000009

Firmware v1.2.8 build0304 (GA)

Mode NAT (Proxy-based)

Licenses (🇺🇸 173.243.138.92)

☒ Subscription License

Proxy/UTM Sessions 0 / 250000

0%

☒ Content Analysis

```
FPX4KET318000009 # diag wad license summary
Available License Seat: 10000
Max Licensed Session: 250000
Current User Count: 0
Current Licensed Session: 0
```

FortiProxy HA - Licensing

- When Working in HA, License is shared between cluster members.
- 50% of the slave licenses are added to the Primary unit.
- License count = Primary unit seat + 50% of Secondary HA member.

```
FPXVM10000150452 # diag wad license
```

```
License Seats Registered:
```

```
FPXVM10000150452: 250
```

```
FPXVM10000150453: 250
```

```
New License Seats Adjusted:
```

```
FPXVM10000150452: 375
```

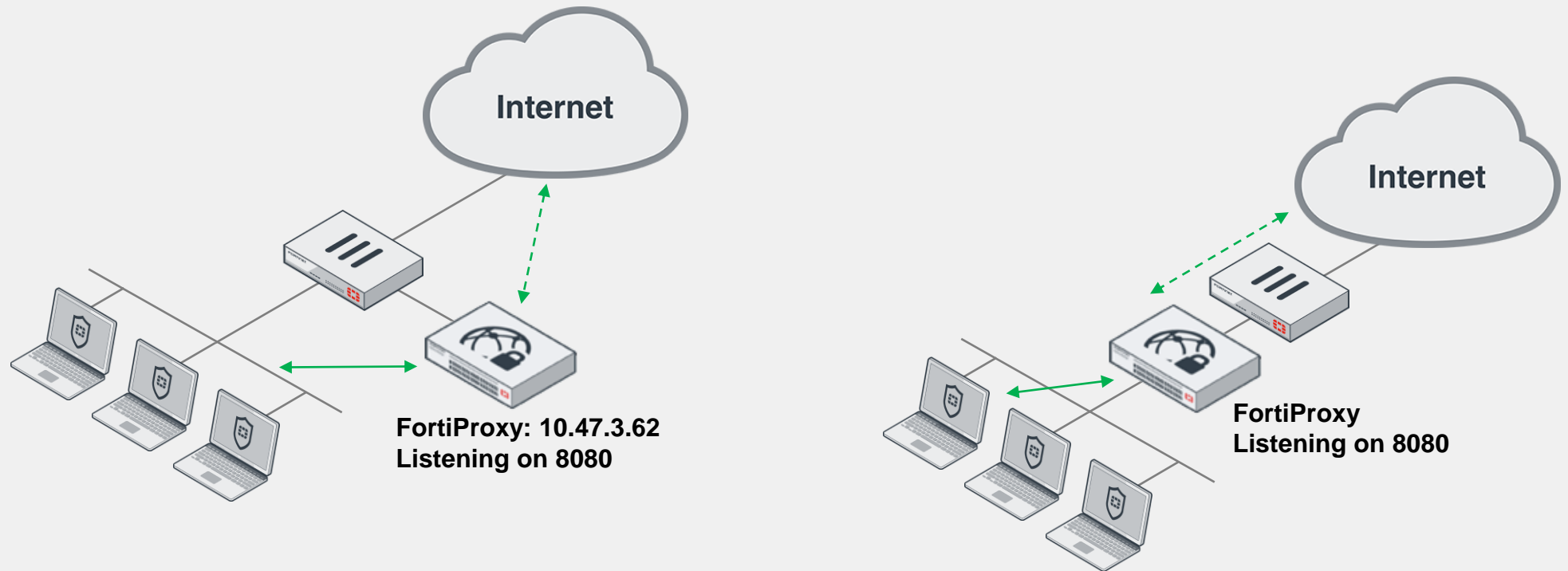
```
FPXVM10000150453: 125
```

```
Available License Seat: 375
```



Deployment modes

Explicit Proxy Deployment



Browser directs HTTP/S traffic to the FortiProxy Explicit Proxy (PAC file Configuration supported).

Explicit Proxy Deployment: pac file

The screenshot displays the FortiGate configuration interface for an Explicit Proxy. The left sidebar shows the navigation menu with 'Proxy Settings' expanded and 'Explicit Proxy' selected. The main configuration area is divided into three sections: 'Proxy Setting', 'Configuration', and 'Proxy Auto Config (PAC)'. The 'PAC Status' is enabled, and the 'PAC Port' is set to 'Use HTTP Port' with a 'Specify' button next to it. The 'PAC File Content' section has an 'Edit' button highlighted with an orange box. A modal window titled 'This Explicit Proxy [web-proxy] is used by policy 3' is open, showing the 'File Content' field with a PAC file script. The script includes rules for bypassing the proxy for specific IP ranges and a default rule for all other traffic. Below the 'File Content' field, there are 'Import' and 'Cancel' buttons. A second modal window titled 'Local Area Network (LAN) Settings' is also open, showing the 'Automatic configuration' section with the 'Use automatic configuration script' checkbox checked and the 'Address' field set to 'http://10.47.3.62:8081/proxy.pac'. The 'Proxy server' section has the 'Use a proxy server for your LAN' checkbox unchecked.

Proxy Settings

- Explicit Proxy
- Web Proxy Setting
- Web Proxy Profile
- Forwarding Server
- Server URL
- FTP Proxy
- Isolator Server

Security Fabric

- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- Content Analyses
- WAN Optimization
- Web Cache
- VPN
- User & Device
- Log & Report

This Explicit Proxy [web-proxy] is used by policy 3

Name: web-proxy

Interfaces: any

Proxy Setting

Status: ☒

HTTP Incoming IP: 0.0.0.0

HTTP Incoming Port: 8080

HTTPS Incoming Port: Use HTTP Port Specify

Configuration

FTP Over HTTP: ☐

SOCKS Proxy: ☐

Prefer DNS Result: IPv4 IPv6

Unknown HTTP Version: Reject Tunnel Best Effort

SEC Default Action: Accept Deny

SSL Algorithm: High Medium Low

Authentication Realm: default

IPv6 Status: ☐

Return to Sender: ☐

Proxy Auto Config (PAC)

PAC Status: ☒

PAC Port: Use HTTP Port Specify 8081

PAC File Content: Edit Download

Maximum File Size: 262144 bytes

File Size: 1119 bytes

File Content:

```
isInNet(dnsResolve(host), "192.168.0.0", "255.255.0.0") ||
isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
return "DIRECT";

// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
if (isInNet(myIpAddress(), "10.194.0.0", "255.255.0.0"))
return "PROXY 10.194.3.62:8080";

// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
return "PROXY 10.194.3.63:8080; PROXY 10.194.3.64:8080";
}
```

Import Browse... No file selected. Import

Cancel

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☒ Use automatic configuration script

Address: http://10.47.3.62:8081/proxy.pac

Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 10.47.3.62 Port: 8080 Advanced

☒ Bypass proxy server for local addresses

OK Cancel

Explicit Proxy Deployment:download pac file

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.194.3.61	10.47.3.62	TCP	66	63053 → 8081 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
2	0.000749	10.47.3.62	10.194.3.61	TCP	66	8081 → 63053 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
3	0.000883	10.194.3.61	10.47.3.62	TCP	54	63053 → 8081 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4	0.001403	10.194.3.61	10.47.3.62	HTTP	288	GET /proxy.pac HTTP/1.1
5	0.001736	10.47.3.62	10.194.3.61	TCP	60	8081 → 63053 [ACK] Seq=1 Ack=235 Win=30720 Len=0
6	0.001901	10.47.3.62	10.194.3.61	HTTP	1282	HTTP/1.1 200 OK (application/x-ns-proxy-autoconfig)

- > Frame 6: 1282 bytes on wire (10256 bits), 1282 bytes captured (10256 bits) on interface 0
- > Ethernet II, Src: 00:45:72:74:05:02 (00:45:72:74:05:02), Dst: 00:45:72:74:04:01 (00:45:72:74:04:01)
- > Internet Protocol Version 4, Src: 10.47.3.62, Dst: 10.194.3.61
- > Transmission Control Protocol, Src Port: 8081, Dst Port: 63053, Seq: 1, Ack: 235, Len: 1228
- > Hypertext Transfer Protocol
- ▼ Line-based text data: application/x-ns-proxy-autoconfig

```
function FindProxyForURL(url, host) {\r\n\r\n    // If the hostname matches, send direct.\r\n    \tif (dnsDomainIs(host, "intranet.domain.com") ||\r\n        \t\tshExpMatch(host, "(*.abcdomain.com|abcdomain.com)"))\r\n        \t\treturn "DIRECT";\r\n\r\n    // If the protocol or URL matches, send direct.\r\n    \tif (url.substring(0, 4)=="ftp:" ||\r\n        \t\tshExpMatch(url, "http://abcdomain.com/folder/*"))\r\n        \t\treturn "DIRECT";\r\n\r\n}
```

Explicit Proxy Deployment: Web Traffic

diagnose wad filter src 10.194.3.61

diagnose wad session list

Session: explicit proxy 10.194.3.61:63176(10.47.3.62:15006)->23.74.131.118:443 id=1189799668
worker=0 vd=0 fw-policy=3

Log & Report	#	Date/Time	Source	Destination	Service	Result	Policy
Forward Traffic	1	11:32:25	10.194.3.61	23.74.131.118	HTTPS	✓ 33.20 kB / 12.72 kB	3 (Allow-ExplicitWebProxy)

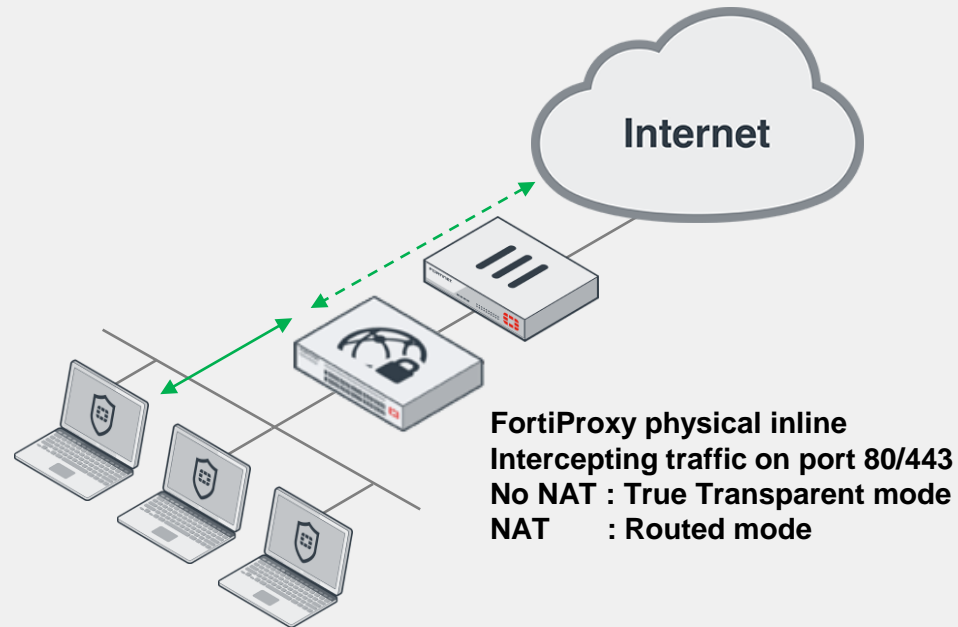
tcp.port==63176 or tcp.port==15006

	Time	Source	Destination	Frame len	Server Name	Info
373	19.662763	10.194.3.61	10.194.3.62	66		63176 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
374	19.662823	10.194.3.62	10.194.3.61	66		8080 → 63176 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024
375	19.663294	10.194.3.61	10.194.3.62	54		63176 → 8080 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
378	19.663728	10.194.3.61	10.194.3.62	269		CONNECT www.ti.com:443 HTTP/1.1
379	19.663749	10.194.3.62	10.194.3.61	54		8080 → 63176 [ACK] Seq=1 Ack=216 Win=30720 Len=0
384	19.903917	10.47.3.62	23.74.131.118	74		15006 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=303823 TSecr=0 WS=1024
386	20.100189	23.74.131.118	10.47.3.62	74		443 → 15006 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4141243177 TSecr=303843
387	20.100265	10.47.3.62	23.74.131.118	66		15006 → 443 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=303842 TSecr=4141243177
388	20.100567	10.194.3.62	10.194.3.61	126		HTTP/1.1 200 Connection established
389	20.101943	10.194.3.61	10.194.3.62	571	www.ti.com	Client Hello
390	20.101978	10.194.3.62	10.194.3.61	54		8080 → 63176 [ACK] Seq=73 Ack=733 Win=31744 Len=0
391	20.102111	10.47.3.62	23.74.131.118	213	www.ti.com	Client Hello
392	20.102476	23.74.131.118	10.47.3.62	66		443 → 15006 [ACK] Seq=1 Ack=148 Win=43776 Len=0 TSval=4141243177 TSecr=303843
400	20.300292	23.74.131.118	10.47.3.62	1598		Server Hello
401	20.300353	10.47.3.62	23.74.131.118	66		[TCP ACKed unseen segment] 15006 → 443 [ACK] Seq=148 Ack=2881 Win=35840 Len=0 TSval=303862 TSecr=4141243177
402	20.300376	23.74.131.118	10.47.3.62	985		[TCP Previous segment not captured] 443 → 15006 [PSH, ACK] Seq=2881 Ack=148 Win=65024 Len=919 TSval=4141243177 TSecr=303843
403	20.300385	10.47.3.62	23.74.131.118	66		[TCP ACKed unseen segment] 15006 → 443 [ACK] Seq=148 Ack=3800 Win=37888 Len=0 TSval=303862 TSecr=4141243177
404	20.306344	10.194.3.62	10.194.3.61	1598		8080 → 63176 [PSH, ACK] Seq=73 Ack=733 Win=31744 Len=1544 [TCP segment of a reassembled PDU]
405	20.306377	10.47.3.62	23.74.131.118	192		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
406	20.307196	10.194.3.61	10.194.3.62	54		[TCP ACKed unseen segment] 63176 → 8080 [ACK] Seq=733 Ack=3519 Win=2102272 Len=0
407	20.326252	10.194.3.61	10.194.3.62	180		[TCP ACKed unseen segment] , Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message



Transparent Proxy Inline Proxy Deployment

- FortiProxy appliance acts as a transparent bridge in the network and analyze client content traversing the device





Transparent Inline Deployment: Web Traffic

diagnose wad filter src 10.194.3.61

diagnose wad session list

Session: transparent proxy 10.194.3.61:63260(10.47.3.63:18166)->104.69.82.240:443

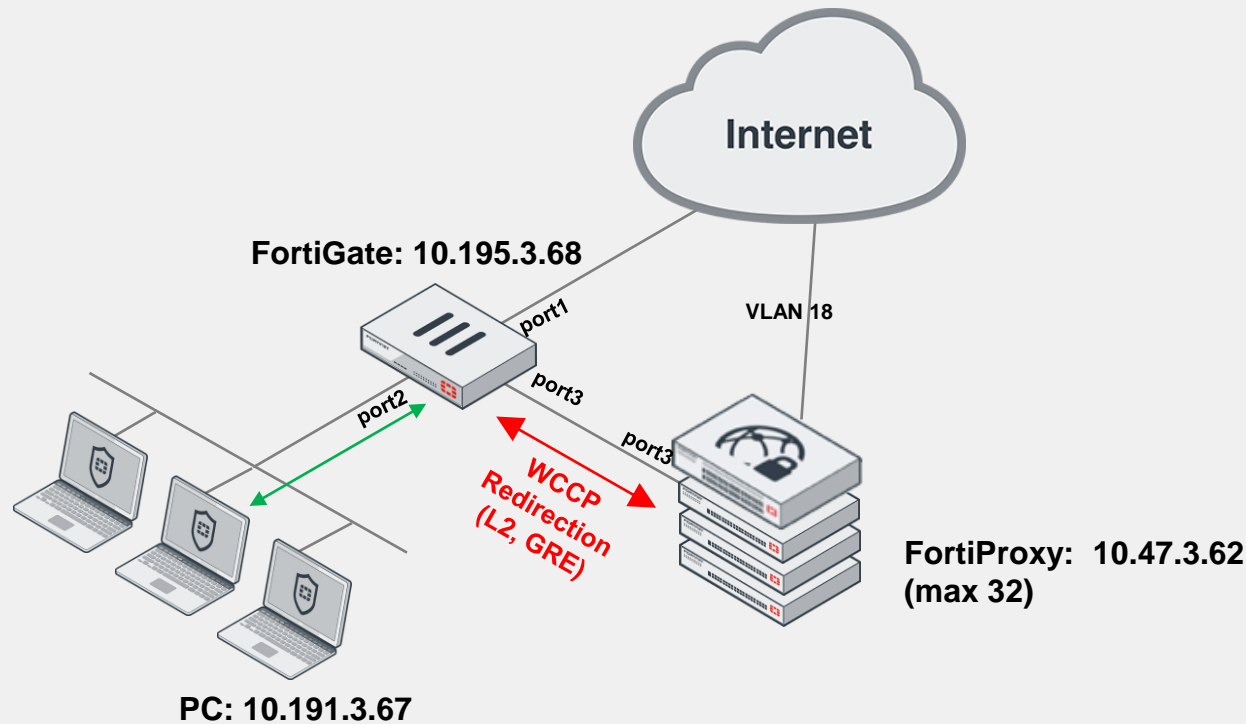
id=1189799778 worker=0 vd=0 fw-policy=2

 Log & Report	#		Date/Time	Source	Destination	Service	Result	Policy
Forward Traffic	1		11:52:13	10.194.3.61	 104.69.82.240	HTTPS	✓ 89.01 kB / 11.70 kB	2 (Intercept-Web-Service)

Time	Source	Destination	Frame len	Server Name	Info
100 9.946397	10.194.3.61	192.168.148.6	70		Standard query 0x89ce A www.ti.com
101 9.946479	10.47.3.63	192.168.148.6	70		Standard query 0x89ce A www.ti.com
102 9.964461	192.168.148.6	10.47.3.63	434		Standard query response 0x89ce A www.ti.com CNAME china.www.ti.com.edgekey.net CNAME china.www.ti.com.edgekey.net
103 9.964510	192.168.148.6	10.194.3.61	434		Standard query response 0x89ce A www.ti.com CNAME china.www.ti.com.edgekey.net CNAME china.www.ti.com.edgekey.net
104 9.969130	10.194.3.61	104.69.82.240	66		63260 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
105 9.969221	104.69.82.240	10.194.3.61	66		443 → 63260 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
108 9.969605	10.194.3.61	104.69.82.240	54		63260 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
110 9.969901	10.47.3.63	104.69.82.240	74		18166 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=426393 TSecr=0 WS=1024
116 9.970927	10.194.3.61	104.69.82.240	571	www.ti.com	Client Hello
117 9.970943	104.69.82.240	10.194.3.61	54		443 → 63260 [ACK] Seq=1 Ack=518 Win=30336 Len=0
138 10.145629	104.69.82.240	10.47.3.63	74		443 → 18166 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=390449804 TSecr=426393 WS=128
139 10.145673	10.47.3.63	104.69.82.240	66		18166 → 443 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=426411 TSecr=390449804
145 10.233453	10.47.3.63	104.69.82.240	213	www.ti.com	Client Hello
146 10.233681	104.69.82.240	10.47.3.63	66		443 → 18166 [ACK] Seq=1 Ack=148 Win=43776 Len=0 TSval=390449804 TSecr=426420
162 10.838250	104.69.82.240	10.47.3.63	1598		Server Hello
163 10.838274	10.47.3.63	104.69.82.240	66		[TCP ACKed unseen segment] 18166 → 443 [ACK] Seq=148 Ack=2881 Win=35840 Len=0 TSval=426480 TSecr=390450496
164 10.838287	104.69.82.240	10.47.3.63	985		[TCP Previous segment not captured] 443 → 18166 [PSH, ACK] Seq=2881 Ack=148 Win=65024 Len=919 TSval=390450496 TSecr=426420
165 10.838292	10.47.3.63	104.69.82.240	66		[TCP ACKed unseen segment] 18166 → 443 [ACK] Seq=148 Ack=3800 Win=37888 Len=0 TSval=426480 TSecr=390450496
166 10.839628	104.69.82.240	10.194.3.61	1598		443 → 63260 [PSH, ACK] Seq=1 Ack=518 Win=30336 Len=1544 [TCP segment of a reassembled PDU]
167 10.839653	10.47.3.63	104.69.82.240	192		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
168 10.840183	10.194.3.61	104.69.82.240	54		[TCP ACKed unseen segment] 63260 → 443 [ACK] Seq=518 Ack=3447 Win=2102272 Len=0
173 10.845442	10.194.3.61	104.69.82.240	180		[TCP ACKed unseen segment] , Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
174 10.845458	104.69.82.240	10.194.3.61	54		[TCP Previous segment not captured] 443 → 63260 [ACK] Seq=3447 Ack=644 Win=30336 Len=0

Transparent Proxy WCCP Deployment


- FortiProxy appliance acts as a transparent bridge in the network and analyze client content traversing the device.
- WCCP can be used to integrate with an existing network architecture and deliver scalability and load balancing. Supports WCCP client and Mask assignment.



WCCP Load distribution supports distribution across multiple devices, with "HERE I AM" and "I SEE YOU" discovery

Transparent Proxy WCCP Deployment: Setting on FortiGate

```
config system settings
    set wccp-cache-engine disable >>FGT act as
wccp router
end
config system interface
    edit "port3" >>To FortiProxy
        set ip 10.195.3.68 255.255.252.0
        set wccp enable
    end
config system wccp
    edit "97" >> Service group id
        set router-id 10.195.3.68
        set server-list 10.195.0.0 255.255.252.0
        set server-type proxy
        set forward-method L2
        set return-method L2
```

 next

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        ....
        set wccp enable >>Redirect
to WCCP Cache (FortiProxy)
    next
end
```

Tips for WCCP Service group:

- use same group id on both side
- Service Group 0 is for only http
- Service Group 5 is for only ftp
- Service Group 70 is for only https
- Available Service Group ID that support dynamic port intercept are 51-255

Transparent Proxy WCCP Deployment: Setting on FortiProxy

```
config system settings
```

```
    set wccp-cache-engine enable >>FPX act as wccp Cache
```

```
end
```

```
config system interface
```

```
    edit "port3" >>To FortiGate
```

```
        set ip 10.195.3.62 255.255.252.0
```

```
        set wccp enable
```

```
end
```

```
config system wccp
```

```
    edit "97"
```

```
        set cache-id 10.195.3.62
```

```
        set router-list "10.195.3.68"
```

```
        set ports-defined destination
```

```
        set ports 80 443
```

```
        set cache-engine-method L2
```

```
next
```



```
config firewall policy
```

```
    edit 4
```

```
        set srcintf "port3"
```

```
        set dstintf "port1"
```

```
        set srcaddr "all"
```

```
        set dstaddr "all"
```

```
        set action accept
```

```
        set schedule "always"
```

```
        set service "HTTP" "HTTPS"
```

```
        set webproxy-profile "Default"
```

```
Next
```

Note: Default Proxy policy type is 'Transparent'

Verify wccp status

```
FGT # diagnose test application wccp 5
```

```
service-97 in vdom-root: installed
```

```
key: ip=10.195.3.62, change-number=1
```

```
cache_list: 1
```

```
0. 10.195.3.62
```

```
primary assignment:
```

```
key=10.195.3.62 change-number=1
```

```
num_routers=1
```

```
router element[0]: router_id=10.195.3.68,  
receive_id=4, ch_no=1
```

```
cache-server-num=1, format=not standard:
```

```
10.195.3.62
```

```
buckets:
```

```
00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00  
00 ...
```

5	11.042687	10.195.3.62	10.195.3.68	178	2.0	Here I am
6	11.042820	10.195.3.68	10.195.3.62	162	2.0	I see you
9	21.038288	10.195.3.62	10.195.3.68	186	2.0	Here I am
10	21.038377	10.195.3.68	10.195.3.62	210	2.0	I see you
12	31.027306	10.195.3.62	10.195.3.68	186	2.0	Here I am
13	31.027364	10.195.3.68	10.195.3.62	210	2.0	I see you
14	36.023422	10.195.3.62	10.195.3.68	378	2.0	Redirect assign
94	41.027873	10.195.3.62	10.195.3.68	186	2.0	Here I am
95	41.027921	10.195.3.68	10.195.3.62	210	2.0	I see you

```
Frame 14: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits)  
Ethernet II, Src: 00:45:72:74:05:03 (00:45:72:74:05:03), Dst: 00:45:72:74:0b:03  
Internet Protocol Version 4, Src: 10.195.3.62, Dst: 10.195.3.68  
User Datagram Protocol, Src Port: 2048, Dst Port: 2048  
Web Cache Communication Protocol
```

```
WCCP Message Type: 2.0 Redirect assign (12)
```

```
WCCP Version (>=2): 0x0200
```

```
Length: 328
```

```
> Security Info
```

```
> Service Info
```

```
▼ Assignment Info
```

```
Type: Assignment Info (6)
```

```
Length: 288
```

```
Assignment Key IP Address: 10.195.3.62
```

```
Assignment Key Change Number: 1
```

```
Number of Routers: 1
```

```
> Router IP: 10.195.3.68
```

```
▼ Number of WC: 1
```

```
WC IP: 10.195.3.62 id: 0
```

```
▼ Buckets
```

```
Bucket 0: 0
```

```
FPX # diagnose test application wccp 6
```

```
service-97 in vdom-root
```

```
erouter_list: 1 routers in total
```

```
0. 10.195.3.68
```

```
receive_id:24 change_number:2
```

```
cache servers seen by this router:
```

```
0. 10.195.3.62 weight:0 (*Designated
```

```
Web Cache)
```



Verify L2 Redirect Traffic-FGT

FGT Debug flow:

```
id=20085 trace_id=10 func=print_pkt_detail line=5727 msg="vd-root:0 received a packet(proto=6, 10.191.3.67:58427->34.104.35.123:80) from port2. flag [S], seq 2481449498, ack 0, win 64240"
```

```
id=20085 trace_id=10 func=init_ip_session_common line=5898 msg="allocate a new session-000021eb"
```

```
id=20085 trace_id=10 func=iprope_dnat_check line=5038 msg="in-[port2], out-[]"
```

```
id=20085 trace_id=10 func=iprope_dnat_check line=5051 msg="result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000"
```

```
id=20085 trace_id=10 func=vf_ip_route_input_common line=2621 msg="find a route: flag=04000000 gw-10.47.7.254 via port1"
```

```
id=20085 trace_id=10 func=iprope_fwd_check line=764 msg="in-[port2], out-[port1], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0"
```

....

```
id=20085 trace_id=10 func=fw_forward_handler line=799 msg="Allowed by Policy-1:"
```

```
id=20085 trace_id=10 func=wccp_output line=297 msg="l2_forward"
```

```
id=20085 trace_id=10 func=wccp_output line=312 msg="send packet via dev-port3"
```



Verify L2 Redirect Traffic-FPX

FPX# diagnose hardware deviceinfo nic port3

Name: port3

...

Hwaddr: 00:45:72:74:05:03 <<

Log & Report		#	Date/Time	Source	Destination	Service	Result	Policy
Forward Traffic		1	11:45:12	10.191.3.67	103.51.64.224	HTTPS	2.42 kB / 1.46 MB	4 (WCCP)
	Time	Source	Destination	Frame len	Server Name	Info		
11	0.644148	10.191.3.67	103.51.64.224	66		65281 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256		
12	0.644230	103.51.64.224	10.191.3.67	66		443 → 65281 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=		
13	0.644974	10.191.3.67	103.51.64.224	54		65281 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0		
14	0.645322	10.191.3.67	103.51.64.224	576	www.rd.go.th	Client Hello		
15	0.645342	103.51.64.224	10.191.3.67	54		443 → 65281 [ACK] Seq=1 Ack=523 Win=30336 Len=0		
16	0.723272	103.51.64.224	10.191.3.67	191		Server Hello, Change Cipher Spec, Encrypted Handshake		
17	0.724535	10.191.3.67	103.51.64.224	105		Change Cipher Spec, Encrypted Handshake Message		
18	0.724566	103.51.64.224	10.191.3.67	54		443 → 65281 [ACK] Seq=138 Ack=574 Win=30336 Len=0		
Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)								
Ethernet II, Src: 00:45:72:74:0b:03 (00:45:72:74:0b:03), Dst: 00:45:72:74:05:03 (00:45:72:74:05:03)								
Destination: 00:45:72:74:05:03 (00:45:72:74:05:03)								
Address: 00:45:72:74:05:03 (00:45:72:74:05:03)								
.... ..0. = LG bit: Globally unique address (factory default)								
.... ..0 = IG bit: Individual address (unicast)								
> Source: 00:45:72:74:0b:03 (00:45:72:74:0b:03)								
Type: IPv4 (0x0800)								
Internet Protocol Version 4, Src: 10.191.3.67, Dst: 103.51.64.224								
Transmission Control Protocol, Src Port: 65281, Dst Port: 443, Seq: 0, Len: 0								

Verify GRE Redirect Traffic

FGT Debug flow:

```
id=20085 trace_id=2 func=print_pkt_detail line=5727 msg="vd-root:0 received a packet(proto=6, 10.191.3.67:65294->40.77.226.250:443) from port2. flag [S], seq 3254445230, ack 0, win 64240"
```

.....

```
id=20085 trace_id=2 func=fw_forward_handler line=799 msg="Allowed by Policy-1:"
```

```
id=20085 trace_id=2 func=wccp_output line=245 msg="gre_forward"
```

```
id=20085 trace_id=2 func=wccp_output line=291 msg="send packet via dev-port3"
```

	Time	Source	Destination	Frame len	Info
1	0.000000	10.191.3.67	40.77.226.250	94	65294 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=
Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)					
Ethernet II, Src: 00:45:72:74:0b:03 (00:45:72:74:0b:03), Dst: 00:45:72:74:05:03 (00:45:72:74:05:03)					
Internet Protocol Version 4, Src: 10.195.3.68, Dst: 10.195.3.62					
Generic Routing Encapsulation (WCCP)					
> Flags and Version: 0x0000					
Protocol Type: WCCP (0x883e)					
▼ Redirect Header					
.... ...0 = Dynamic Service: Well-known service					
.... ..0. = Alternative bucket used: Primary bucket used					
.... .0.. = WCCP Redirect header is valid: Header contents are valid					
Service ID: Unknown (97)					
Alternative Bucket: 0					
Primary Bucket: 125					
Internet Protocol Version 4, Src: 10.191.3.67, Dst: 40.77.226.250					
Transmission Control Protocol, Src Port: 65294, Dst Port: 443, Seq: 0, Len: 0					

GRE Encap

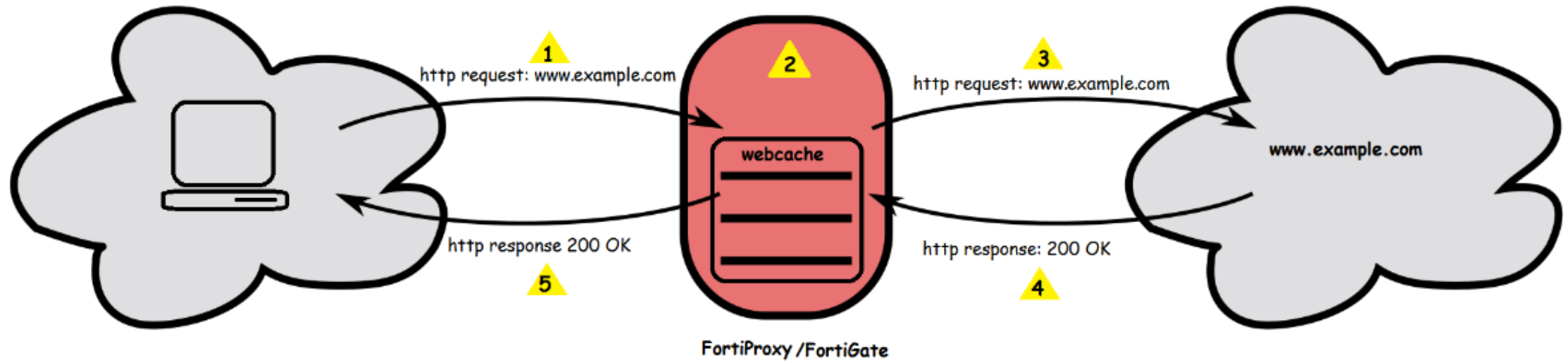
Real Web traffic





Understanding Web Proxy flow

Web Proxy Flow



Webproxy Traffic flow

Use the following debugging command to display the HTTP flow for Explicit Proxy Service:

```
# diagnose wad debug enable category http
```

```
# diagnose wad debug enable category policy
```

```
# diagnose wad debug enable level info
```

```
# diagnose wad debug show
```

Category: http policy

Level: info

NOTE: category ALL **not recommend** as it might cause High CPU on wad



1. Receive an HTTP request from the client:

```
[0x7ff98710b050] Received request from client: 192.168.244.4:2052
```

```
GET http://www.example.com/ HTTP/1.1
```

```
Accept: text/html, application/xhtml+xml, */*
```

```
Accept-Language: en-US
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Accept-Encoding: gzip, deflate
```

```
Host: www.example.com
```

2. FortiProxy sends a DNS request for www.example.com / or check Cache content/ check Web filter category/action

```
[0x7ff98710b050] DNS request name=www.example.com len=10 type/pref=0/0
```

3. FortiProxy sends an HTTP request to the www.example.com server:

```
[0x7ff98710b050] Connect to server: 184.29.23.193:80
```

```
[0x7ff98710b050] Forward request to server:
```

```
GET / HTTP/1.1
```

```
Accept: text/html, application/xhtml+xml, */*
```

```
Accept-Language: en-US
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Accept-Encoding: gzip, deflate
```

```
Host: www.example.com
```

```
DNT: 1
```

```
Connection: Keep-Alive
```

4. FortiProxy receives an HTTP response from the server:

[0x7ff98710b050] Received response from server:

HTTP/1.1 200 OK

Server: Apache

Last-Modified: Thu, 07 Mar 2019 16:52:00 GMT

ETag: "e0e1-58383ecc76c00"

Accept-Ranges: bytes

Content-Encoding: gzip

X-Frame-Options: SAMEORIGIN

Content-Type: text/html; charset=UTF-8

X-Akamai-Transformed: 9 - 0 pmb=mTOE,2

Date: Thu, 28 Mar 2019 02:06:48 GMT

Content-Length: 10427

Connection: keep-alive



5. FortiProxy forwards the HTTP response to the client:

[0x7ff98710b050] Forward response from server:

HTTP/1.1 200 OK

Server: Apache

Last-Modified: Thu, 07 Mar 2019 16:52:00 GMT

ETag: "e0e1-58383ecc76c00"

Accept-Ranges: bytes

Content-Encoding: gzip

X-Frame-Options: SAMEORIGIN

Content-Type: text/html; charset=UTF-8

X-Akamai-Transformed: 9 - 0 pmb=mTOE,2

Date: Thu, 28 Mar 2019 02:06:48 GMT

Content-Length: 10427



Webproxy Traffic flow

Sample wad debug #1 : 504 Gateway Timeout (DNS)

[0x7fae0f12a1d0] Received request from client: 192.168.244.4:51481

GET http://www.nonexist123.com/ HTTP/1.1

Host: www.nonexist123.com

....

[0x7fae0f12a1d0] DNS request name=www.nonexist123.com len=19 type/pref=0/0

wad_http_client_read_sync(27334): state=3 clt->pause=1 ret=1

[0x7fae0f12a1d0] **DNS resolved: N/A**

__wad_http_build_replmsg_resp(18135): Generating replacement message. DNS error

[0x7fae0f12a1d0] Forward response from cache:

HTTP/1.1 504 Gateway Timeout

Content-Type: text/html

Cache-Control: no-cache

504 DNS look up failed

The webserver reported that an error occurred while trying to access the website. Please click [here](#) to return to the previous page.

URL: <http://www.nonexist123.com/>

User name:

Group name:



Steps to troubleshoot

- Ping from FortiProxy to url:

```
#execute ping www.nonexist123.com
Unable to resolve hostname.
```

- Check reachability to DNS server:

```
# execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=7.0 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=7.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=7.2 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.0/7.2/7.4 ms
```

- Run packet capture for dns traffic while try to ping to url again:

```
# diagnose sniffer packet any 'host 8.8.8.8 and port 53' 6 0 1
interfaces=[any]
filters=[host 8.8.8.8 and port 53]
2021-11-08 20:43:03.145012 port1 out 10.47.2.122.1120 -> 8.8.8.8.53: udp
37
```

No.	Time	Source	Destination	Frame len	Info
1	0.000000	10.47.2.122	8.8.8.8	79	Standard query 0x80b6 A www.nonexist123.com
2	0.014670	8.8.8.8	10.47.2.122	152	Standard query response 0x80b6 No such name A www.nonexist123.com SOA a.gtld-servers.net



Webproxy Traffic flow

Sample wad debug #2 : 504 Gateway Timeout (No response from the server)

[0x7f5cf37f13d0] Received request from client: 192.168.244.139:49331

GET http://www.nonexist123.com/ HTTP/1.1

[0x7f5cf37f13d0] DNS request name=www.nonexist123.com len=19 type/pref=0/0

wad_http_client_read_sync(27334): state=3 clt->pause=1 ret=1

[0x7f5cf37f13d0] DNS resolved: 1.2.3.4

wad_http_request_policy_set(24453): match pid=260 **policy-id=559** vd=0 in_if=10, out_if=10 192.168.244.139:49331 ->1.2.3.4:80

[0x7f5cf37f13d0] Connect to server: 1.2.3.4:80

wad_http_forward_request_start(15294): http session 0x7f5cf3894ed0 req=0x7f5cf37f13d0 connecting

.....

__wad_http_trap_port_close(12275): trap port event close

__wad_http_build_replmsg_resp(18135): Generating replacement message. 504 error

wad_http_client_notify(19118): @@@ http client 0x7f5cf3894ed8 resume_read=0

wad_http_send_cache_resp(16708): req=0x7f5cf37f13d0 body_expect=0

[0x7f5cf37f13d0] Forward response from cache:

HTTP/1.1 504 Gateway Timeout

Content-Type: text/html

504 Gateway Timeout: remote server did not respond to the proxy

The webserver reported that an error occurred while trying to access the website. Please click [here](#) to return to the previous page.

URL: http://www.nonexist123.com/

User name:

Group name:



Steps to troubleshoot

- Run packet capture for traffic between FortiProxy and server while try to access url from client:

```
# diagnose sniffer packet any 'host <FortiProxy wan ip> or host  
<Server IP>' 60  
interfaces=[any]  
filters=[<FortiProxy wan ip> or <Server IP>]
```

- Tips: How to know server ip:

```
# diagnose test application dnsproxy 7  
vfid=0, name=www.ti.com, ttl=20:18:1798  
23.199.87.15 (ttl=20) <<<<<
```

- If there's multiple ip, please collect packet capture with all ip and keep running below command during test to match client/server tcp port:

```
# diagnose wad session list  
Session: explicit proxy 10.96.1.128:56509(10.91.167.148:59820) ->  
23.199.87.15:443
```



Web server ip: Port

Client ip:port

FortiProxy ip:Port

Sample wad debug #3 : *Block by Web Filter*

[0x7f5cf37f0a10] Received request from client: 192.168.244.139:49331

GET http://www.hotmail.com/ HTTP/1.1

[0x7f5cf37f0a10] DNS request name=www.hotmail.com len=15 type/pref=0/0

wad_http_client_read_sync(27334): state=3 clt->pause=1 ret=1

[0x7f5cf37f0a10] DNS resolved: 204.79.197.212

wad_http_request_policy_set(24453): match pid=260 policy-id=559 vd=0 in_if=10, out_if=10 192.168.244.139:49331->204.79.197.212:443

wad_url_filter_req_alloc(822): url_req=0x7f5cf3946f30 id=52

wad_http_client_read_sync(27334): state=3 clt->pause=1 ret=1

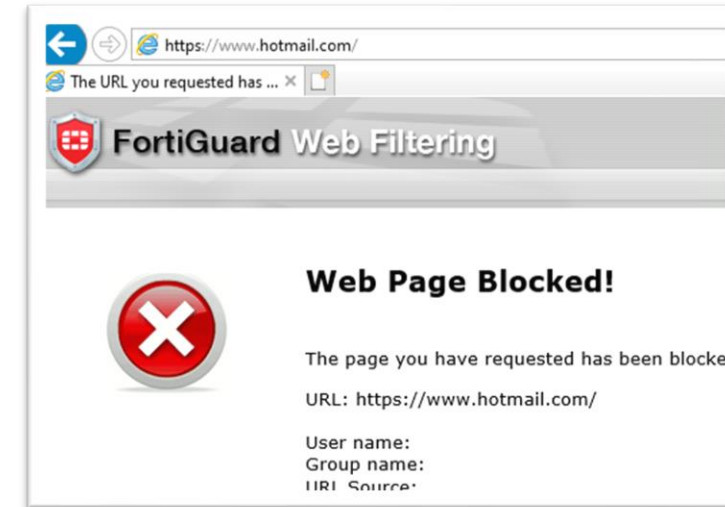
wad_url_cat_find(1479): url right-away category not hit: is_ip=0 url/ip=0/0

wad_url_filter_check_url_filter_on_result(2602): get result id=52 cate=23 action=ftgd-block warn_domain=0 warn_session=0

__wad_http_build_replmsg_resp(18135): Generating replacement message. FTGD blocked

[0x7f5cf37f0a10] Forward response from cache:

HTTP/1.1 403 Forbidden



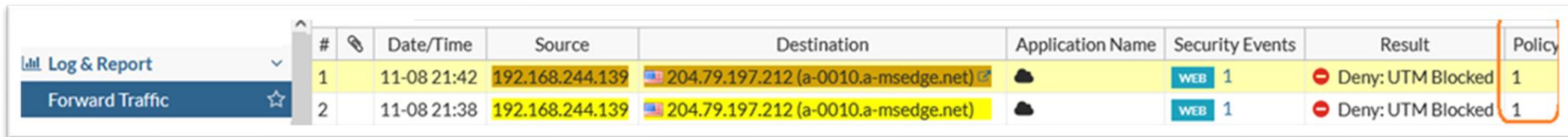
Step to troubleshoot

Check setting on Matching policy, from wad debug, from traffic log and from Policy test.

- Wad debug:

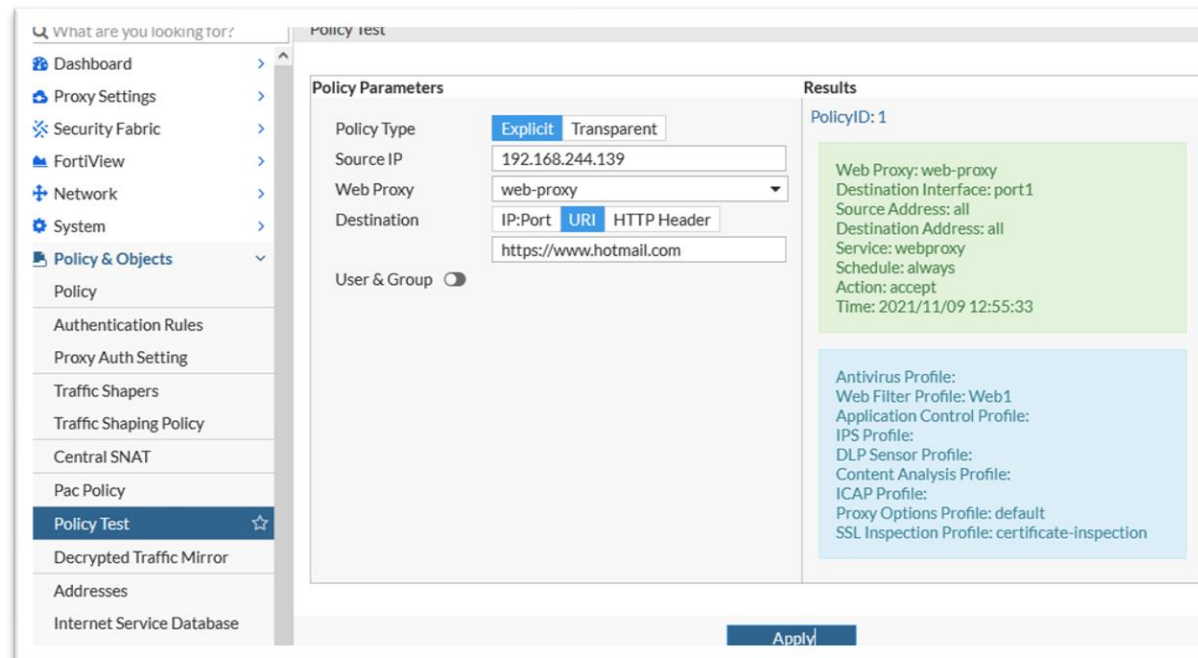
```
wad_http_request_policy_set(24453): match pid=260 policy-id=559 vd=0 in_if=10,  
out_if=10 192.168.244.139:49331->204.79.197.212:443
```

- Traffic log:



#	Date/Time	Source	Destination	Application Name	Security Events	Result	Policy
1	11-08 21:42	192.168.244.139	204.79.197.212 (a-0010.a-msedge.net)	WEB	1	Deny: UTM Blocked	1
2	11-08 21:38	192.168.244.139	204.79.197.212 (a-0010.a-msedge.net)	WEB	1	Deny: UTM Blocked	1

- Policy Test:



What are you looking for?

- Dashboard
- Proxy Settings
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
 - Policy
 - Authentication Rules
 - Proxy Auth Setting
 - Traffic Shapers
 - Traffic Shaping Policy
 - Central SNAT
 - Pac Policy
 - Policy Test
 - Decrypted Traffic Mirror
 - Addresses
 - Internet Service Database

Policy test

Policy Parameters

Policy Type: ☒ Explicit ☐ Transparent

Source IP: 192.168.244.139

Web Proxy: web-proxy

Destination: IP:Port ☒ URI ☐ HTTP Header

https://www.hotmail.com

User & Group: ☐

Results

PolicyID: 1

Web Proxy: web-proxy
Destination Interface: port1
Source Address: all
Destination Address: all
Service: webproxy
Schedule: always
Action: accept
Time: 2021/11/09 12:55:33

Antivirus Profile:
Web Filter Profile: Web1
Application Control Profile:
IPS Profile:
DLP Sensor Profile:
Content Analysis Profile:
ICAP Profile:
Proxy Options Profile: default
SSL Inspection Profile: certificate-inspection

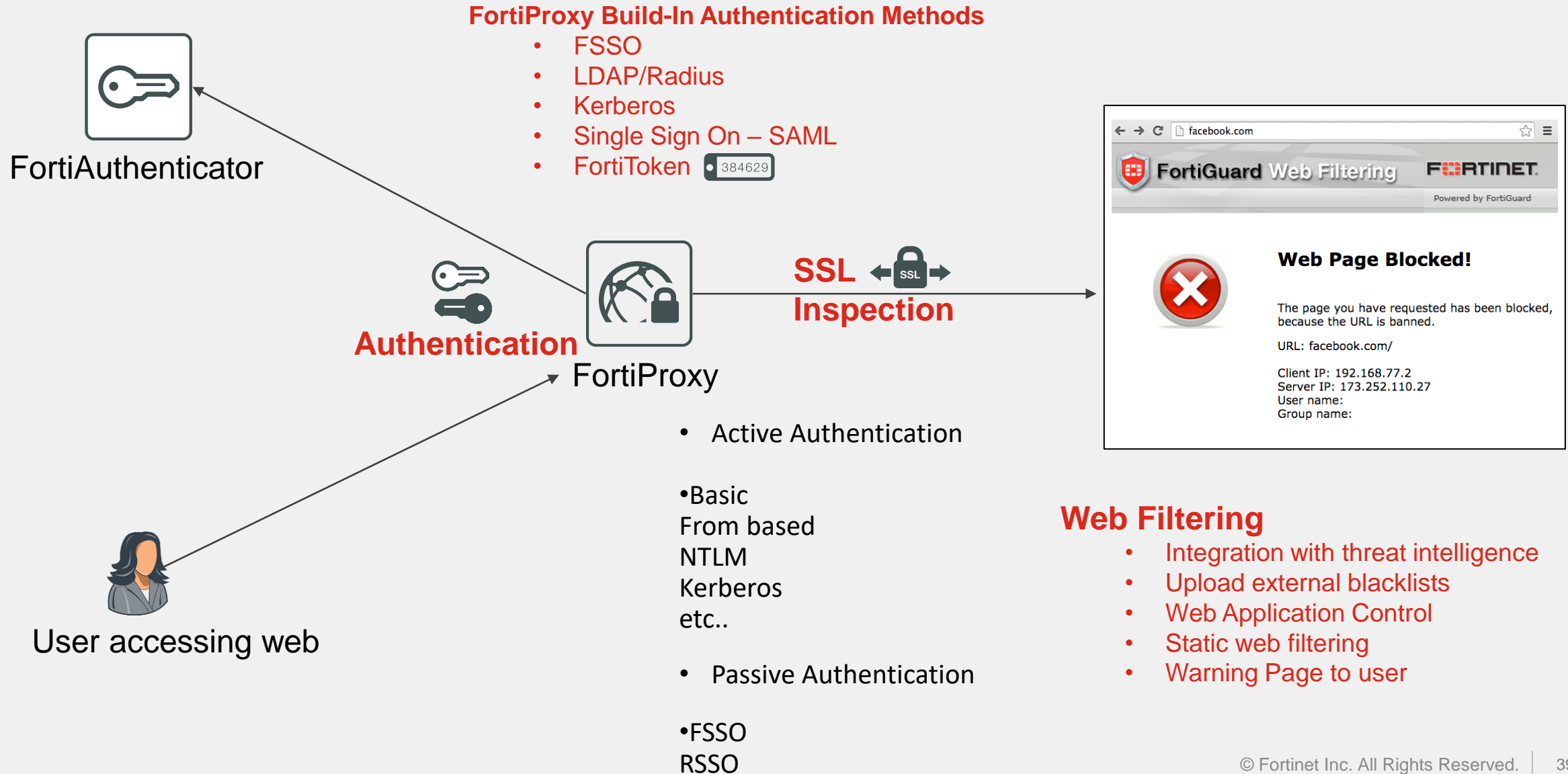
Apply



Authentication and Authorization



Acceptable Use Policy Enforcement



Authentication

Authentication Types:

Active Authentication

Basic
From based
NTLM
Kerberos
etc..

Passive Authentication

FSSO
RSSO

Configuration Includes

Authentication Scheme (User Database Source)

Authentication rules.

Users/Groups.

Firewall policies.

The screenshot displays the FortiProxy-4000E configuration interface. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main panel is divided into two sections: 'Edit Authentication Scheme' and 'Edit Rule'.

Edit Authentication Scheme:

- Name: LDAP
- Method: Basic
- User database: DC
- FSSO guest: ☐

Edit Rule:

- Name: All_Users
- Protocol: HTTP
- Source Interface: port3
- Source Address: all
- Source IPv6 Address: +
- Destination IPv6 Address: +
- Destination Address: all
- Authentication Scheme: ☒ LDAP
- IP-based Authentication: ☐ Enable ☐ Disable
- SSO Authentication Scheme: ☐
- Comments: Write a comment... 0/1023
- Enable This Rule: ☐ Enable ☐ Disable

Group List:

Group Name	Group Type	Members
All_Users	Firewall	DC 0
Guest-group	Firewall	guest 0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)	0

Policy List:

Name	Source	Destination	Schedule	Service	Action
Explicit-Web →web-proxy →port1	INET	all	always	webproxy	ACCEPT
Implicit	all	all			



Troubleshooting Authentication issues.

List / Clear Authenticated users.

```
# diagnose wad user list
# diagnose firewall auth list
# diagnose wad user clear << clear authenticated users.
```

FortiProxy-4000E # diag wad user list

```
ID: 4, VDOM: root, IPv4: 10.203.7.4
user name   : fortinet
worker      : 48
duration    : 9
auth_type   : IP
auth_method : Basic
pol_id      : 0
g_id        : 0
user_based  : 0
expire      : no
LAN:
  bytes_in=94809 bytes_out=1552168
WAN:
  bytes_in=2972954 bytes_out=151008
```

List User group membership for IP based / FSSO users.

```
# diagnose test application wad 2400 << switch to informer daemon
# diagnose test application wad 110
```

List FSSO User database synchronized from the Collector agent

```
# diagnose debug authd fsso list
```



Troubleshooting Authentication issues.

Debug commands to troubleshoot Authentication issues.

Webproxy Authentication debug.

```
# diag wad deb enable category auth
# diag deb en
```

Radius / LDAP (authentication

```
# diag deb app fnbamd -1 ** (LDAP authentication only when "ldap-user-cache" is disabled)
# diag deb en
```

Packet sniffer.

```
# diag sniffer packet any 'host User_IP' 6 0 1
```

```
# diag sniffer packet any 'host Authentication_Server' 6 0 1
```



Troubleshooting Authentication issues.

When using Session based Authentication:

```
config authentication rule
    edit "All_Users"
        set ip-based disable
        set web-auth-cookie enable
    next
end
```

Note : web-auth Cookie is available only with session-based authentication. i.e., IP based authentication disabled.

This setting reduces authentication requests for existing sessions, which makes NTLM authentication more scalable.

Troubleshooting Authentication issues.

LDAP User Cache – Long time cache

```
config web-proxy global
    set ldap-user-cache enable >> enable by default
end
```

When the LDAP user cache is enabled FortiProxy uses Long time Cache, the group cache is kept 15 days for inactivity and uses background refreshing to fetch server-side changes

Clearing the Cache

```
diagnose test application wad 2500 << switch to user-information daemon
diagnose test application wad 160 << clear cached user info mapping table
diagnose test application wad 157 << clear cached SID mapping table
```



Performance issues

Performance issue on FortiProxy

diag sys top-mem ← List top processes by memory usage

```
ipshelper (3747): 177732kB
node (3724): 159605kB
miglogd (3816): 151949kB
miglogd (3824): 151210kB
miglogd (3745): 150447kB
```

diag sys top 1 99

Run Time: 0 days, 22 hours and 40 minutes
16U, 0N, 4S, 63I, 8WA, 0HI, 9SI, 0ST; 32110T, 6701F

		Name of the process		CPU usage	Memory usage
wad	1471	S	24.7	1.3	4
wad	1472	R	23.7	1.3	8
wad	11873	S	19.8	1.1	2
wad	1474	S	18.8	1.4	5
wad	1475	R	18.8	1.3	2
wad_csvc_cs	1452	S	4.4	0.9	15
ipsengine	1650	S <	3.9	0.7	8

wad: responsible for Webproxy / Proxy inspection / web cache & Wan optimization services

wad_csvc_cs: the central Caching daemon that maintains the in-memory cached objects. And consuming around 20% of memory is consider normal



Performance issue on FortiProxy

```
# get sys perf status
```

```
CPU states: 14% user 3% system 0% nice 65% idle 9% iowait 0% irq 9% softirq
```

Overall CPU usage

```
CPU0 states: 15% user 4% system 0% nice 77% idle 0% iowait 0% irq 4% softirq
```

```
CPU1 states: 5% user 1% system 0% nice 81% idle 0% iowait 0% irq 13% softirq
```

```
CPU2 states: 6% user 1% system 0% nice 89% idle 0% iowait 0% irq 4% softirq
```

```
CPU3 states: 21% user 4% system 0% nice 60% idle 0% iowait 0% irq 15% softirq
```

```
CPU4 states: 9% user 2% system 0% nice 86% idle 0% iowait 0% irq 3% softirq
```

```
CPU5 states: 12% user 2% system 0% nice 80% idle 0% iowait 0% irq 6% softirq
```

```
CPU6 states: 20% user 3% system 0% nice 70% idle 0% iowait 0% irq 7% softirq
```

CPU usage per core

```
Memory: 32880948k total, 13923920k used (42.3%), 6955908k free (21.2%), 12001120k freeable (36.5%)
```

```
Average network usage: 38432 / 55769 kbps in 1 minute, 46470 / 62205 kbps in 10 minutes, 47504 / 65250 kbps in 30 minutes
```

```
Maximal network usage: 67436 / 77805 kbps in 1 minute, 124226 / 112866 kbps in 10 minutes, 124226 / 126075 kbps in 30 minutes
```

```
Average sessions: 52974 sessions in 1 minute, 52837 sessions in 10 minutes, 50262 sessions in 30 minutes
```

```
Maximal sessions: 55892 sessions in 1 minute, 59093 sessions in 10 minutes, 59093 sessions in 30 minutes
```

```
Average session setup rate: 1204 sessions per second in last 1 minute, 1236 sessions per second in last 10 minutes, 1271 sessions per second in last 30 minutes
```

```
Maximal session setup rate: 1400 sessions per second in last 1 minute, 1940 sessions per second in last 10 minutes, 1940 sessions per second in last 30 minutes
```

```
Virus caught: 0 total in 1 minute
```

```
IPS attacks blocked: 0 total in 1 minute
```

```
Uptime: 0 days, 23 hours, 40 minutes
```

Tips:

- Freeable memory = reclaimable
- Look for CPU utilization per CPU core.

>>>"freeable":memory which can be released under system pressure.

So, the actual free memory is around 57% in this example >>>>>



Check load for each wad worker vs CPU/memory usage

```
# diagnose wad license detail
```

```
Purchased License Seat: 2500
```

```
Available License Seat: 2500
```

```
Max Licensed Session: 62500
```

```
Current User Count: 234
```

```
Current Licensed Sessions: 444
```

```
Max bypassed Sessions: 0
```

```
Session counts:
```

	licensed	bypassed	total licensed
worker 0:	41	0	107663
worker 1:	64	0	111616
worker 2:	55	0	118094
worker 3:	61	0	104250
worker 4:	77	0	114735
worker 5:	38	0	116261
worker 6:	64	0	105668
worker 7:	44	0	97908
total:	444	0	876195

```
# diagnose test application wad 1000
```

```
Process [0]: WAD manager type=manager(0) pid=1778 diagnosis=yes.
```

```
Process [1]: type=dispatcher(1) index=0 pid=2434 state=running
```

```
diagnosis=no debug=enable valgrind=unsupported/disabled
```

```
Process [2]: type=worker(2) index=0 pid=2436 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [3]: type=worker(2) index=1 pid=2437 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [4]: type=worker(2) index=2 pid=2438 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [5]: type=worker(2) index=3 pid=15110 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [6]: type=worker(2) index=4 pid=2440 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [7]: type=worker(2) index=5 pid=2441 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [8]: type=worker(2) index=6 pid=2442 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [9]: type=worker(2) index=7 pid=2443 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [10]: type=algo(3) index=0 pid=2431 state=running
```

```
diagnosis=no debug=enable valgrind=unsupported/disabled
```

```
Process [11]: type=informers(4) index=0 pid=2428 state=running
```

```
diagnosis=no debug=enable valgrind=unsupported/disabled
```

```
Process [12]: type=user-info(5) index=0 pid=2433 state=running
```

```
diagnosis=no debug=enable valgrind=supported/disabled
```

```
Process [13]: type=debug(8) index=0 pid=2427 state=running
```

```
diagnosis=no debug=enable valgrind=unsupported/disabled
```

```
Process [14]: type=config-notify(9) index=0 pid=2430 state=running
```

```
diagnosis=no debug=enable valgrind=unsupported/disabled
```



Additional Diagnosis commands for Performance issues

`diag debug enable`

`diag sys top-summary "-s mem -n 20"`

`diag sys session count`

`diag sys session list`

`diag hardware sysinfo memory`

`diag hardware sysinfo slab`

`diag wad stats summary`

`diag wad session list`

`diag wad license detail`

`diagnose wad memory stats misc`

`diagnose wad stats summary`

`diagnose wad worker tcp stats`

`diagnose wad worker ssl stats`

`diagnose wad worker tunnel stats`

`diagnose wad worker webcache stats`

`diagnose wad csvc webcache stats`

`diagnose wad csvc webcache lists`

`diagnose wacs stats`

`diagnose wad worker bytecache stats`

`diagnose wad csvc bytecache stats`

`diagnose wad csvc bytecache lists`

`diagnose wadbd stats`

`diagnose wad worker memcache stats`

`diagnose wad csvc memcache stats`

`diagnose debug crashlog read`

`diag wad memory report`



Other resources

<https://docs.fortinet.com/product/fortiproxy/7.0>

<https://tools.ietf.org/id/draft-wilson-wrec-wccp-v2-01.txt>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD44578>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD42352>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD42333>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD43824>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD51936>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46113>

FortiProxy and Basic setup: <https://www.youtube.com/watch?v=OiYRsJck2u0>



FAQ

Q: The clients show pop up "Connecting to proxy server for outlook.office365.com" by authen from Fortiproxy. How I can fix it?

A: If you not intend to authenticate this flow, then you can bypass authentication by use Authentication Rule.

Q: How do we know how many user is currently used user license?

A: From Web access Dashboard>License or from CLI: diagnose wad license summary

Q: Can we do a filter in 'diag wad debug enable all' to a specific source ip/dest ip so that not all logs are displayed ?

A: You can use #diag wad filter src/dst x.x.x.x to filter based on source or destination

FORTINET®